AdvanceBB5 and AdvanceUFS User's Manual

Introduction:

This software manual is applicable for both AdvanceBB5 and AdvanceUFS boxes. AdvanceBB5 and AdvanceUFS have the same features and functionalities. The only main difference is that AdvanceBB5 is a Stand-Alone Interface as compared to AdvanceUFS which requires a supplementary UFS Box Interface for RS-232 connection purposes.

In this User's Manual, both AdvanceBB5 and AdvanceUFS are collectively referred to as the AdvanceBOX Interface.

Special Features:

The AdvanceBB5 and AdvanceUFS or collectively known as the AdvanceBOX Interface is a new breed of BB5 TP Unlocking Box and is the first of it's kind to support “Intelligent Learning Mode” which is currently not available in any other BB5 unlocking boxes in the market.

The main Advantage of “Intelligent Learning Mode” is that the End-Users can add additional phone support by themselves without waiting for any software updates from the Product Supporters. AdvanceBOX's “Intelligent Learning Mode” is implemented in the Hardware Level which means that is very stable and reliable as compared to the any software implementation of the same technology.

What is Intelligent Learning Mode?...

To put it in more simpler terms, Intelligent Learning Mode is DK's BB5 Unlocking Theory implemented in the Logic Level (CPLD Implementation). This means that Intelligent Learning Mode will try to HACK and UNLOCK the phone for you using algorithms and techniques prepared by the Product Supporters of AdvanceBOX.

In short, there is a “hacker” inside that AdvanceBOX Interface that will do all the work for you so that you can add new phones in your support list.

Limitations for Intelligent Learning Mode:

Intelligent Learning Mode is only applicable to BB5 phones that uses a NOR Flash for it's primary firmware storage. The reason for this is that BB5 phones that uses a NAND Flash for it's primary firmware storage is also using a new Security Measure which prevents the current TP Unlocking Method from working.

Package Options:

<u>AdvanceBB5 Stand-Alone Box Package:</u>

1 x AdvanceBB5 Box Interface
1 x USB A to USB B Cable
1 x TP Cable
3 x USB DKU-X Pop-Port Type Connectors

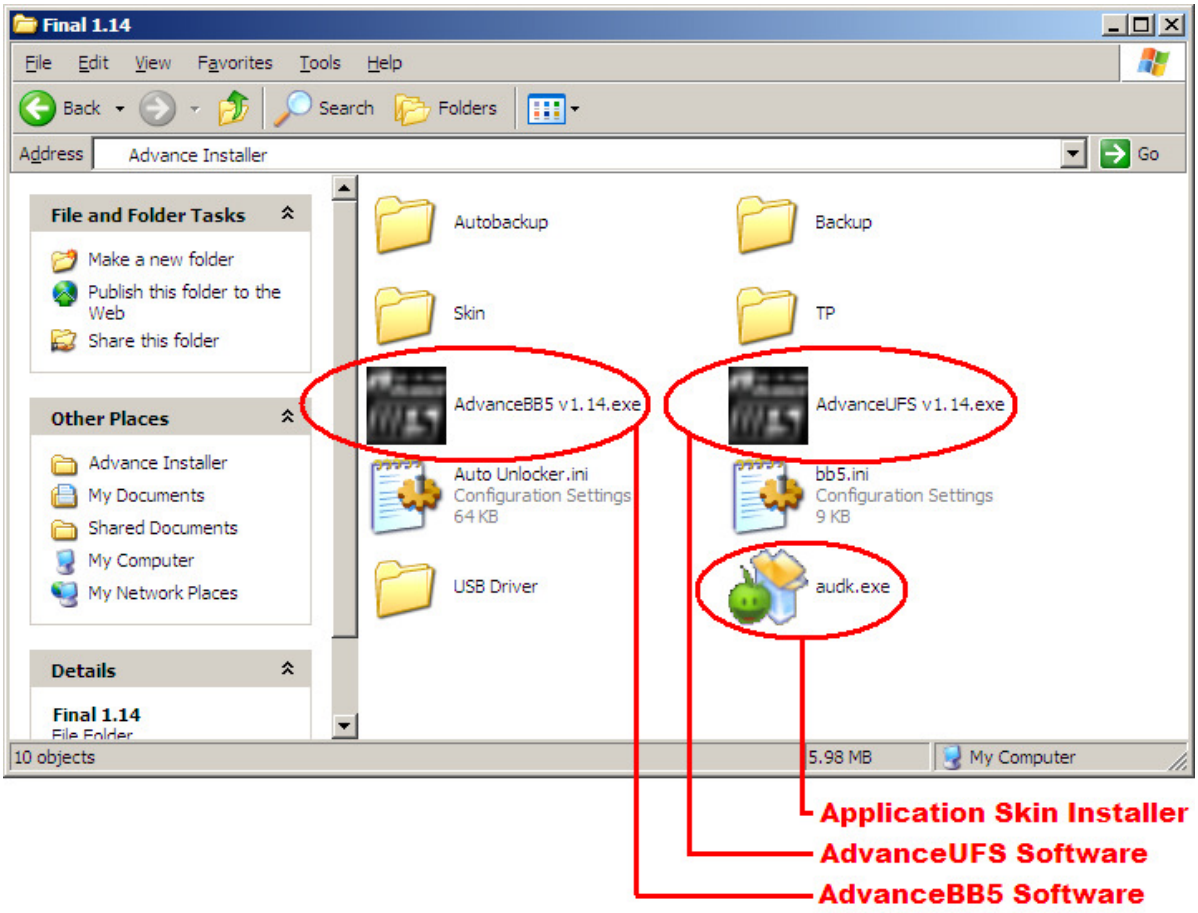
<u>AdvanceUFS Box Package (Requires UFS Box Interface):</u>

1 x AdvanceUFS Box Interface
1 x RJ-45 to RJ-45 1:1 Cable
1 x TP Cable
3 x USB DKU-X Pop-Port Type Connectors

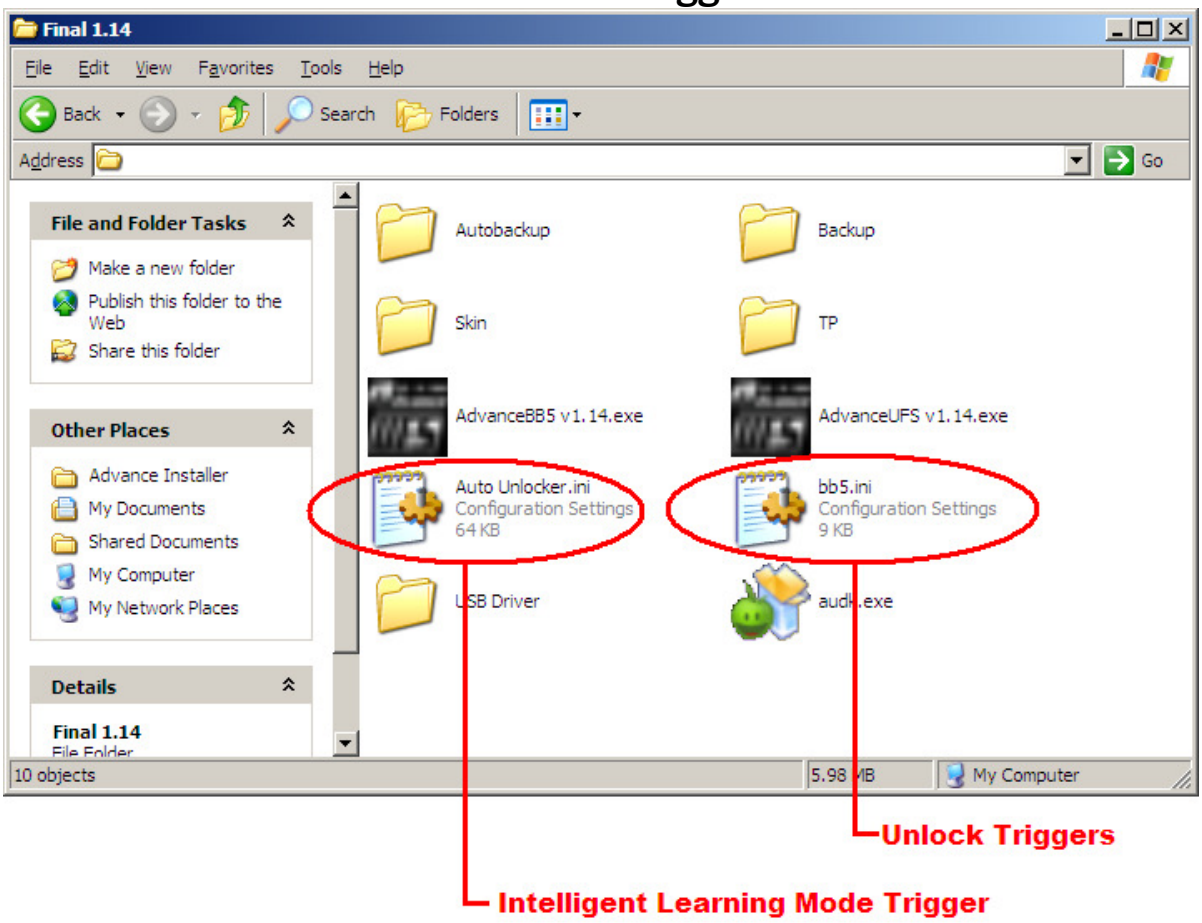
Software Installation:

1. Download the latest Software Version from the support area of www.advance-box.com
2. Make the necessary USB or UFS connections and Install the necessary USB Drivers (AdvanceBB5 USB driver or UFS USB Driver).
3. Install audk.exe Application Skin Installer (used for cosmetic purposes only).

The EXECUTABLE Files:



The BB5 Unlock Trigger Files:



bb5.ini –

Contains BB5 unlock triggers used for unlocking BB5 Phones.
Each unlock trigger is composed of 12-bytes.
Any manual changes done to the unlock triggers inside bb5.ini will invalidate the unlock triggers.

The bb5.ini can be updated in 3 ways:

1. Self-Update using Intelligent Learning Mode…
2. Trigger Sharing Updates – Get Unlock triggers from the AdvanceBOX Sub-Forum in http://www.gsmcity.de … The Unlock Triggers Made by "Intelligent Learning Mode" can be shared with other users of AdvanceBOX Interfaces. (direct link to AdvanceBOX sub-forum: http://www.gsmhosting.com/vbb/forumdisplay.php?f=444)
3. Wait for Product Supporters to release an updated bb5.ini

Auto Unlocker.ini -

Contains important firmware information for "Intelligent Learning Mode" Function.

The Auto Unlocker.ini can only be updated by the Product Supporters. Please check the Support section in http://www.advance-box.com for updates in the Auto Unlocker.ini

The Software Interface

Read Phone – Displays the information about the IMEI, Firmware Version and Lock Status of the BB5 Phone connected to the AdvanceBOX Interface.

Backup 308 – Makes a backup of PM 308 for safekeeping.

Restore 308 – Restores PM 308 backups.

SP Unlock – Disables SP-LOCKS using Test-Point Unlocking.

Factory Reset – Restores Factory Settings (User Code = 12345).

Rd Full PM – Makes a backup of all valid PM Seems.

Wr Full PM – Restores full PM backups.

Abort – Terminates current operation.

Show TP – Displays the correct Test-Point connections for the BB5 Phone connected to the AdvanceBOX Interface.

Save Log – Saves a LOG file for all operations done.

KP/FBUS – Manually selects KeyPress PSW instead of the default FBUS PSW. KeyPress PSW is still sent through FBUS Frames so you don't need to manually enter the codes in the phone's keypad.

Allow Bad IMEI – Allows SP-Unlocking for phones with bad IMEI eg: 1234567...

Select AD – Manually Selects NOR Flash ADDRESS PIN for Test-Point.

Quick SP-Unlocking Guide

1. Disassemble the BB5 Phone you wish to unlock and perform the necessary tasks to reveal the Test-Points on the the Phone's PCB.
2. Connect the AdvanceBOX Interface to your PC through the USB Port if you are using the AdvanceBB5 Stand-Alone Interface or through the UFS Box RJ-45 port if you are using the AdvanceUFS Interface.
3. Execute AdvanceBB5.exe if you are using the AdvanceBB5 Stand-Alone Interface or AdvanceUFS.exe if you are using the AdvanceUFS Interface.
4. Connect the TP-Cable to the RJ-45 port of your AdvanceBOX Interface.
5. Attach the correct DKU-X USB cable to the FEMALE USB port of the TP-Cable. Do not connect the DKU-X to the USB port of your PC as this connection type is not yet supported.
6. Connect the DKU-X Pop-Port interface to the Pop-Port of the BB5 Phone you wish to Unlock.
7. Attach the BLACK “slip-clip” connector to the GND Battery Terminal of the BB5 Phone.
8. Attach the YELLOW “slip-clip” connector to the BSI Battery Terminal of the BB5 Phone.
9. Attach the RED “slip-clip” connector to the POSITIVE (+) Battery Terminal of the BB5 of the BB5 Phone.
10. Attach the BLACK “alligator-clip” connector to a GND Point near the RAP3G or the Flash Chip.
11. Power Up the phone by pressing the “tact-switch” for 3 seconds or by using a Tweezer if the “tact-switch” is not available on the Phone's PCB.
12. On the Software Interface, click “Read Phone” to check if the phone is properly connected.
13. On the Software Interface, tick “Show TP” to see the Correct Test-Point connections required for the Phone.
14. On the Software Interface, click “SP-Unlock” to begin the Unlocking Process. The “SP-Unlock” button will automatically create a PM 308 backup of the Phone if the Phone still has no PM 308 backup.
15. When the Software Interface prompts you to Connect the Test-Points (TP), you must first Connect the BLACK “tp-pin” (CLK) to the Phone's PCB, then proceed to Connect the YELLOW “tp-pin” (ADX) to the Phone's PCB.

*** If unlock triggers are available for the Phone's Firmware Version and Flash Chip Type, SP-Unlocking will take less than 5 seconds.

*** If unlock triggers are NOT available for the Phone's Firmware Version and Flash Chip Type, SP-Unlocking will automatically enter “Intelligent Learning Mode” and the Sp-Unlocking Process will take more than 5 seconds.

The BLACK and YELLOW “tp-pins” should be connected at all times during the entire SP-Unlocking Process. Failure to properly connect the “tp-pins” at all times will result to SP-Unlock Failure.

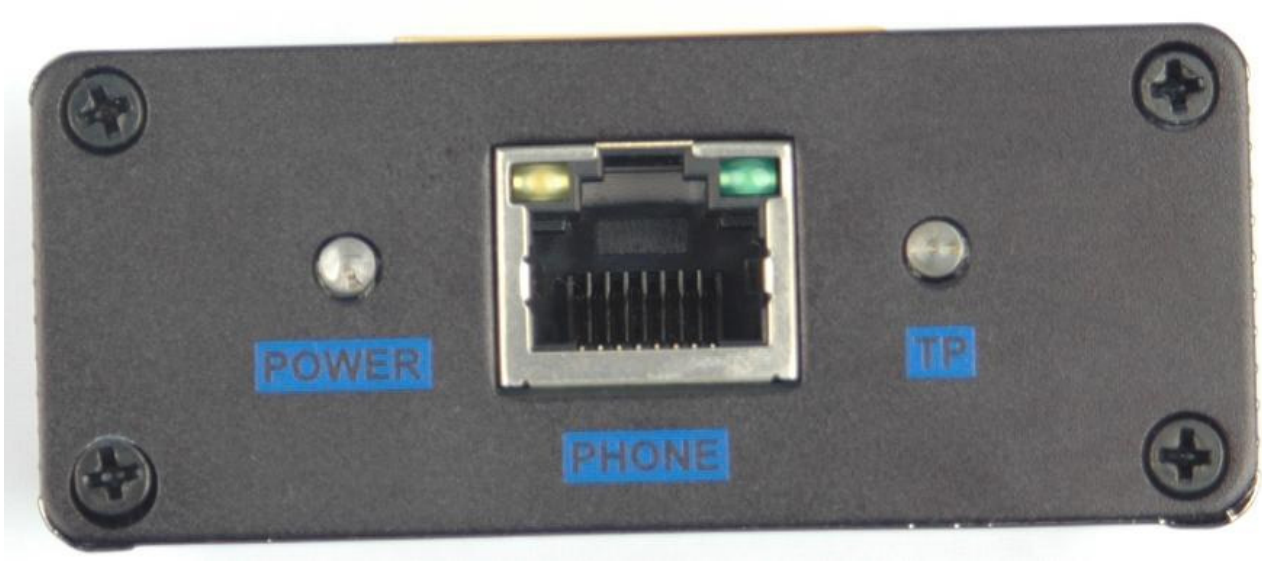
In an event of a SP-Unlocking Failure, just repeat steps 14 and 15.

If the Phone prematurely shuts off during the Intelligent Learning Mode:

1. **Disconnect the TP connection and the RED “slip-clip” connector from the POSITIVE (+) Battery Terminal.**
2. **Reconnect the RED “slip-clip” connector, Power Up the phone and reconnect the TP CLOCK then ADX.**

The AdvanceBB5 Stand-Alone Interface

The Front Panel



Power – 5v Power Indicator
Phone – RJ—45 Port for TP-Cable (Yellow LED = TX, Green LED = RX)
TP – Test-Point Connection Indicator

The Back Panel

USB – Connect directly to the PC's USB Port and not through a USB Hub in order to get 500mA for N95, 8600 and 7390 Phones.

*** If the AdvanceBB5 Stand-Alone Interface is connected through a BUS Powered USB Hub, proper Operation of the device is not guaranteed.

*** If the AdvanceBB5 Stand-Alone Interface is connected through a Self-Powered USB Hub or a USB Hub with an External Power source, then proper Operation “may” be guaranteed.

*** If the AdvanceBB5 Stand-Alone Interface is connected through the PC's Root USB Hub, then proper operation IS GUARANTEED.

The AdvanceUFS Interface

The Front Panel

ON – 5v Power Indicator
TP CABLE – RJ—45 Port for TP-Cable
TP – Test-Point Connection Indicator

The Back Panel

ACP-X – OPTIONAL External Power supply using ACP-8X or ACP-12X Chargers.
UFS – RJ—45 Port for UFS Box Connection.

*** ACP-X OPTIONAL External Power is only required for 400mA phones such as N95, 8600 and 7390. For any other BB5 phone, EXTERNAL POWER IS NOT REQUIRED.

*** The AdvanceUFS Interface can achieve OPTIMAL Performance when ACP-X is NOT CONNECTED. You must only use an ACP-X External Charger ONLY if the Phone is not powering up properly due to lack of mA given by the UFS Box.

The TP-Cable Set

Special TP-Cable Features:

1. Three GND Points:
   a. Pop-Port GND Required (1st Ground Point)
   b. Battery Interface Optional GND (2nd Ground Point)
   c. Alligator Clip Optional GND (3rd Ground Point)
2. Compatible with any DKU-X USB that comes with BB5 Phone Package. For new BB5 Phones with new Pop-Port interface, just use the USB cable that came with the Phone Package. Therefore there is no need to buy additional TP-Cables when new BB5 Phones are released.
3. Correct "tp-pins" cable length and thickness for maximum "pulsing" effect. (15cm @ 10-15 degrees shift phase)

Safety Precautions

1. Always connect any of the three GND points to the Phone's PCB before making any NON-GND connections such as Battery BSI, Battery Positive (+), TP CLOCK and TP ADX.
2. For the AdvanceBB5 Interface, only use ACP-X External Power if the Phone cannot power up properly due to lack of mA from the UFS Box.
3. Always opt to work in a Static-Free environment.
4. Avoid touching the metallic “tp-pins” of the TP-Cable with your bare fingers.
5. NEVER Modify the TP-Cables and NEVER use TP-Cables designed for other BB5 Unlocking tools.
6. Always check the Battery Terminal Connections before powering the Phone. The standard BB5 battery connection is POSITIVE, BSI then GND from left to right. However, some phones such as N95, 8600 and 7390 have a different battery connection which is POSITIVE, GND then BSI. The correct battery interface can be found in the Battery of the BB5 Phone. POSITVE and GND are marked properly in the Battery's sticker and BSI is the unmarked connection.

Software Interface Error Messages

Waiting for phone to response...

Problem:
If this message shows up for more than 5 seconds, it means that the phone is no longer in powered up.

Solution:
1. DO NOT PRESS ABORT BUTTON
2. Disconnect the Test-Point connections (Black and Yellow “tp-pins”)
3. Disconnect the RED “slip-clip” Positive (+) Battery Terminal Connection
4. Reconnect the RED “slip-clip” Positive (+) Battery Terminal Connection
5. Power Up the Phone
6. Reconnect BLACK “tp-pin” CLOCK
7. Reconnect YELLOW “tp-pin” ADX

>>> Please connect TP

Problem:
If this message shows up even if you are 100% sure that you have properly made the correct TP Connections, it means that the phone is no longer in powered up.

Solution:
8. DO NOT PRESS ABORT BUTTON
9. Disconnect the Test-Point connections (Black and Yellow “tp-pins”)
10. Disconnect the RED “slip-clip” Positive (+) Battery Terminal Connection
11. Reconnect the RED “slip-clip” Positive (+) Battery Terminal Connection
12. Power Up the Phone
13. Reconnect BLACK “tp-pin” CLOCK
14. Reconnect YELLOW “tp-pin” ADX

SP Data Corrupted….
RPL calculation needed to fix SP lock certificate

Problem:
SP Data is corrupted, therefore SP-Unlock is not possible

Solution:
Make RPL request from a 3rd Party BB5 RPL provider to fix the SP Data, then unlock the phone

Firmware/Version not Supported

Problem:
You get this message when trying to unlock a Phone in Learning Mode

Solution:
Leave a message in the support forum so that the Product Supporters can check or update the Auto Unlocker.ini to support your phone

Process Unsuccessful..Try again…

Problem:
You get this message when trying to unlock a Phone in Learning Mode

Solution:
1. Check TP Connections because maybe CLK and ADX are swapped
2. Leave a message in the support forum so that the Product Supporters can check or update the bb5.ini to support your phone (you must specify the Flash Chip used)

Official Support Website
http://www.advance-box.com

Official Support Forum
http://www.gsmhosting.com/vbb/forumdisplay.php?f=444